

Amendments to claims

- 1 1. (Amended) A dynamic file access control and management system configured to access one or  
2 more content sources including a set of content files, said system comprising:
  - 3 A a proxy system linked to said one or more content sources, said proxy system  
4 comprising an access control module configured to selectively obtain ~~a file~~  
5 content comprising data blocks from said content sources as a function of an  
6 authorization of a user requesting said content file and a set of access policies;
  - 7 B. a rights management module configured to generate a set of usage rights  
8 associated with said content file as a function of a set of predefined usage policies  
9 associated with said content file for said user;
  - 10 C. at least one client device having a client module configured to interface to a client  
11 operating system kernel, said client module configured to enforce the set of usage  
12 rights within the operating system kernel ~~selectively inhibit operating system~~  
13 ~~functions with respect to said file as a function of said usage rights~~; and
  - 14 D. one or more communication means, via which said content file and said usage  
15 rights are provided to said client device.
- 1 2. (Amended) The system according to claim 1, wherein said content file and said usage rights  
2 are provided to said client device via different communication means.
- 1 3. (Amended) The system according to claim 1, wherein said files are content includes static  
2 content files.

1       4. (Amended) The system according to claim 1, wherein said ~~files are content includes~~ dynamic  
2            content files.

1       5. (Twice Amended) The system according to claim 1, wherein said communication means  
2       includes a secure transform configured to encrypt and encapsulate said content file into a  
3       message as a function of a session ID and said client is configured to extract said content file  
4       from said message.

1       6. (Amended) The system according to claim 1, wherein said proxy system further includes a  
2       user interface, configured to facilitate creation and editing of said access policies and said usage  
3       policies and association of said access policies and said usage policies with said content files.

1       7. (Previously presented) The system as in claim 1, wherein said client device is a device from a  
2       group comprising:

- 3           1)       a personal computer;
- 4           2)       a workstation;
- 5           3)       a personal digital assistant;
- 6           4)       an e-mail device;
- 7           5)       a cellular telephone;
- 8           6)       a Web enabled appliance; and
- 9           7)       a server.

1       8. (Original) The system of claim 1, wherein said proxy system and at least one of said content  
2       sources are hosted on the same computing device.

1 9. (Amended) A method of dynamic ~~file~~ access control and management of content, the method  
2 comprising:

- 3 A. to ~~each of a set of files~~ content comprising data blocks accessible from a set of  
4 content sources by a proxy system, correlating one or more user and/or client  
5 device identifications and defining a set of usage policies, wherein for ~~a given file~~  
6 the content said usage policies relate to selectively enabling or disabling  
7 operations associated with said content file;
- 8 B. by said proxy system, generating a set of usage rights associated with the content  
9 ~~a target file~~ as a function of a the set of usage policies associated with said ~~target~~  
10 file content and a the one or more user and/or client device identification;
- 11 C. communicating said ~~target file content~~ and said usage rights to a client device  
12 associated with one or more user and/or client device identification; and
- 13 D. using a client module at said client device and configured to interface to a client  
14 operating system kernel, selectively inhibiting enforcing the set of usage rights  
15 within the operating system kernel functions with respect to said target file as a  
16 function of said usage rights.

1 10. (Amended) The method of claim 9, wherein in step C, said communicating is accomplished  
2 by communicating said content target file and said usage rights to said client device via different  
3 communication means.

1 11. (Amended) The method of claim 9, wherein said content set of files includes static content  
2 files.

1 12. (Amended) The method of claim 9, wherein said content set of files includes dynamic  
2 content files.

1 13. (Amended) The method of claim 9, wherein said communicating is accomplished using a  
2 communication means that includes a secure transform, including encrypting and encapsulating  
3 said ~~target file content~~ into a message as a function of a session ID and said client device is  
4 configured to extract said ~~target file content~~ from said message.

1       14. (Amended) The method of claim 9, wherein said proxy system further includes a user  
2       interface and step A include creating and/or editing said access policies and said usage policies  
3       and associating said access policies and said usage policies with said ~~set of files~~ content using  
4       said user interface.

1       15. (Previously presented) The method of claim 9, wherein said client device is a device from a  
2       group comprising:

3               1)       a personal computer;  
4               2)       a workstation;  
5               3)       a personal digital assistant;  
6               4)       an e-mail device;  
7               5)       a cellular telephone;  
8               6)       a Web enabled appliance; and  
9               7)       a server.

1       16. (Previously presented) The method of claim 9, further comprising hosting said proxy system  
2       and at least one content source on the same computing device.